Exhibit D

AO 93 (Rev. 12/09) Search and Seizure Warrant

UNITED STATES DISTRICT COURT

for the

Eastern District of Virginia

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)
Electronic Devices Previously Seized from the Premises of 200 East 39th Street, Apartment 8C, New York, NY 10016

Case No. 1:17-SW-243

UNDER SEAL

SEARCH AND SEIZURE WARRANT

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search of the following person or property located in the Eastern District of Virginia
(identify the person or describe the property to be searched and give its location):

Electronic devices located at a U.S. Government facility in Herndon, Virginia

The person or property to be searched, described above, is believed to conceal *(identify the person or describe the property to be seized)*:

SEE ATTACHMENT A

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property.

YOU ARE COMMANDED to execute this warrant on or before May 24, 2017
(not to exceed 14 days)

☑ in the daytime 6:00 a.m. to 10 p.m. ☑ at any time in the day or night as I find reasonable cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to United States Magistrate Judge Michael S. Nachmanoff.
(name)

☐ I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized *(check the appropriate box)* ☐ for _____ days *(not to exceed 30)*.

☐ until, the facts justifying, the later specific date of _____.

Date and time issued: 5/10/17 @ 12:00 pm

/s/
Michael S. Nachmanoff
United States Magistrate Judge
Judge's signature

City and state: Alexandria, Virginia Michael S. Nachmanoff, United States Magistrate Judge
Printed name and title

A TRUE COPY, TESTE:
CLERK, U.S. DISTRICT COURT

BY _____
DEPUTY CLERK

AO 93 (Rev. 12/09) Search and Seizure Warrant (Page 2)

Return

Case No.: 1:17-SW- ____	Date and time warrant executed:	Copy of warrant and inventory left with:

Inventory made in the presence of :

Inventory of the property taken and name of any person(s) seized:

Certification

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.

Date: _____

_____
Executing officer's signature

_____
Printed name and title

Attachment A

I. Devices to be Searched—Subject Devices

The devices to be searched (the "Subject Devices") include any and all electronic devices seized pursuant to a search warrant executed on or about March 15, 2017 at the premises described as apartment 8C in a building located at 200 East 39th Street, New York, New York 10016.

II. The Search of the Subject Devices

A. Evidence, Fruits, and Instrumentalities of the Child Pornography Offenses

The Subject Devices may be searched for the following evidence, fruits, and/or instrumentalities of violations of Title 18, United States Code, Sections 2252 (activities relating to material constituting or containing child pornography) and 2252A (possession, transportation, receipt, distribution, production, and reproduction of sexually explicit material relating to children) (the "CP Offenses"):

- Evidence of computer programs used to access, transmit, or store information relating to the CP Offenses;
- Evidence of counter-forensic programs (and associated data) that are designed to eliminate data from computer devices, storage media, and related electronic equipment;
- Evidence of visual or written depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256(2);
- Motion pictures, films, videos, and other recordings of visual or written depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256(2);
- Correspondence and records pertaining to violation of the CP Offenses including, but not limited to electronic mail, chat logs, electronic messages, and records bearing on the production, reproduction, receipt, shipment, orders, requests, trades, purchases, or transactions involving any visual depiction of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256(2);
- Records or other items which evidence ownership, control, or use of, or access to computer devices, storage media, and related electronic equipment used to access, transmit, or store information relating to the CP Offenses, including but not limited to sales receipts, warranties, bills for internet access, registry entries, configuration files, saved usernames and passwords, user profiles, email contacts, and photographs.

- Information or correspondence pertaining to affiliation with any child exploitation bulletin boards, chat forums, or organizations;

- Any child pornography as defined by 18 U.S.C. § 2256(8);

- Any child erotica, defined as suggestive visual depictions of nude minors which do not constitute child pornography as defined by 18 U.S.C. § 2256(8) or visual depictions of minors engaged in sexually explicit conduct as defined by 18 U.S.C. § 2256(2);

- Notes, documents, records, invoices, or correspondence, in any format and medium, including, but not limited to, e-mail messages, chat logs and electronic messages, other digital data files and web cache information, related to the possession, distribution, receipt, or production of, or access with intent to view, child pornography as defined in 18 U.S.C. § 2256(8), or visual depictions of minors engaged in sexually explicit conduct as defined in 18 U.S.C. § 2256(2);

- Names, and lists of names and addresses of individuals (including minors) related to the possession, distribution, receipt, or production of, or access with intent to view, child pornography as defined in 18 U.S.C. § 2256(8), or visual depictions of minors engaged in sexually explicit conduct as defined in 18 U.S.C. § 2256(2);

- Mailing lists and/or supplier lists related to the possession, distribution, receipt, or production of, or access with intent to view, child pornography as defined in 18 U.S.C. § 2256(8), or visual depictions of minors engaged in sexually explicit conduct as defined in 18 U.S.C. § 2256(2); and

- Financial records, including credit card information, bills, and payment records related to related to the possession, distribution, receipt, or production of, or access with intent to view, child pornography as defined in 18 U.S.C. § 2256(8), or visual depictions of minors engaged in sexually explicit conduct as defined in 18 U.S.C. § 2256(2).

B. Evidence, Fruits, and Instrumentalities of the Copyright Offenses

The Subject Devices may also be searched for the following evidence, fruits, and/or instrumentalities of violations of violations of 17 U.S.C. § 506 and 18 U.S.C. § 2319 (criminal infringement of a copyright) (the "Copyright Offenses"):

- Evidence of computer programs used to transmit or store information relating to the Copyright Offenses;

- Evidence of counter-forensic programs (and associated data) that are designed to eliminate data from computer devices, storage media, and related electronic equipment;

- Evidence of copyrighted works, including motion pictures, films, videos, other recordings, and documents relating to the Copyright Offenses;

- Correspondence and records pertaining to violation of the Copyright Offenses including, but not limited to electronic mail, chat logs, electronic messages, and records bearing on the transmission, receipt, and/or storage of copyrighted works;

- Records or other items which evidence ownership, control, or use of, or access to computer devices, storage media, and related electronic equipment used to transmit or store information relating to the Copyright Offenses, including but not limited to sales receipts, warranties, bills for internet access, registry entries, configuration files, saved usernames and passwords, user profiles, email contacts, and photographs.

- Any copyrighted works;

- Notes, documents, records, invoices, or correspondence, in any format and medium, including, but not limited to, e-mail messages, chat logs and electronic messages, other digital data files and web cache information, related to the transmission, receipt, and/or storage of copyrighted works;

- Names, and lists of names and addresses of individuals (including minors) related to the transmission, receipt, and/or storage of copyrighted works;

- Mailing lists and/or supplier lists related to the transmission, receipt, and/or storage of copyrighted works; and

- Financial records, including credit card information, bills, and payment records related to the transmission, receipt, and/or storage of copyrighted works.

C. Review of ESI

In conducting a review of ESI on the Subject Devices, law enforcement personnel may use various techniques, including but not limited to:

- surveying various file "directories" and the individual files they contain (analogous to looking at the outside of a file cabinet for the markings it contains and opening a drawer believed to contain pertinent files);

- opening or cursorily reading the first few "pages" of such files in order to determine their precise contents;

- scanning storage areas to discover and possibly recover recently deleted files;

- scanning storage areas for deliberately hidden files;

- performing key word searches through all electronic storage areas to determine whether occurrences of language contained in such storage areas exist that are intimately related to the subject matter of the investigation; and

- making reasonable efforts to utilize computer search methodology to search only for files, documents, or other electronically stored information within the categories identified in Section II.A of this Attachment.

Law enforcement personnel will make reasonable efforts to search only for files, documents, or other electronically stored information within the categories identified in Section II.A and II.B. of this Attachment. However, law enforcement personnel are authorized to conduct a complete review of all ESI from the Subject Devices if necessary to evaluate its contents and to locate all data responsive to the warrant.

UNITED STATES DISTRICT COURT

for the

Eastern District of Virginia

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)
Electronic Devices Previously Seized from the Premises of 200 East 39th Street, Apartment 8C, New York, NY 10016

Case No. 1:17-SW-243

UNDER SEAL

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

Electronic devices located at a U.S. Government facility in Herndon, Virginia,

located in the Eastern District of Virginia, there is now concealed *(identify the person or describe the property to be seized)*:

SEE ATTACHMENT A

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. 2252	Possession and production of sexually explicit material relating to children;
18 U.S.C. 2252A	Activities relating to material containing child pornography;
17/18 U.S.C. 506/2319	Criminal infringement of a copyright

The application is based on these facts:

SEE ATTACHED AFFIDAVIT

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Reviewed by AUSA/SAUSA:
AUSA Neil Hammerstrom

Garrett L. Igo
Applicant's signature

Garrett L. Igo, FBI Special Agent
Printed name and title

Sworn to before me and signed in my presence.

Date: 05/10/2017

/s/
Michael S. Nachmanoff
United States Magistrate Judge
Judge's signature

City and state: Alexandria, Virginia

Michael S. Nachmanoff, United States Magistrate Judge
Printed name and title

IN THE UNITED STATES DISTRICT COURT FOR THE

EASTERN DISTRICT OF VIRGINIA

Alexandria Division

IN THE MATTER OF THE SEARCH OF:	)	**UNDER SEAL**
Electronic Devices Previously Seized from the	)	
Premises of 200 East 39th Street, Apartment 8C,	)	Case No. 1:17-SW-243
New York, NY 10016	)	

AFFIDAVIT IN SUPPORT OF A SEARCH AND SEIZURE WARRANT

I, Garrett L. Igo, being duly sworn, hereby deposes and says:

I. Introduction

A. Affiant

1. I am a Special Agent of the Federal Bureau of Investigation ("FBI") assigned to the New York Field Office, and I have been so employed by the FBI since 2011. I am currently assigned to a squad responsible for counterespionage matters and have worked in the field of counterintelligence from 2011 to present. In the course of my duties as a Special Agent, I am responsible for investigating offenses involving espionage and related violations of law, including unauthorized retention, gathering, transmitting or losing classified documents or materials; unauthorized removal and retention of classified documents or materials; illegally acting in the United States as a foreign agent; other national security offenses; and the making of false statements. As a result of my involvement in espionage investigations and investigations involving the unauthorized disclosure or retention of classified information, as well as my training in counterintelligence operations, I am familiar with the tactics, methods, and techniques of United States persons who possess, or have possessed a United States Government security clearance and may choose to harm the United States by misusing their access to classified information. I am also

familiar, though my training and experience, with the use of computers in criminal activity and the forensic analysis of electronically stored information.

2. I make this Affidavit in support of an application pursuant to Rule 41 of the Federal Rules of Criminal Procedure for a warrant to search the electronic devices specified below ("Subject Devices") for the items and information described in Attachment A. Specifically, and as discussed in detail below, the Subject Devices were previously seized and searched pursuant to a separate warrant defined herein as the "Schulte Search Warrant," and which was issued in connection with an investigation into the unlawful dissemination of classified materials.

3. While searching the Subject Devices for evidence, fruits, and instrumentalities of the offenses set forth in the Schulte Search Warrant, law enforcement officers encountered what appears to be an image of child pornography on one of the Subject Devices. Upon discovery of this suspected image of child pornography, the FBI promptly contacted the Assistant United States Attorneys involved in this investigation to inform them of this development, and the decision was made to seek additional authorization under Rule 41 of the Federal Rules of Criminal Procedure to search the Subject Devices for evidence, fruits, and instrumentalities of offenses involving child pornography, as specified below.

4. Similarly, while searching the Subject Devices for evidence, fruits, and instrumentalities of the offenses set forth in the Schulte Search Warrant, law enforcement officers also encountered what appears to be evidence of copyright infringement—specifically, the illegal streaming of dozens of movies—on one of the Subject Devices. Upon discovery of this evidence, the FBI also promptly contacted the Assistant United States Attorneys involved in this investigation to inform them of this development, and the decision was made to seek additional authorization under Rule 41 of the Federal Rules of Criminal Procedure to search the Subject

Devices for evidence, fruits, and instrumentalities of offenses involving copyright infringement, as specified below.

5. This Affidavit is based upon my personal knowledge; my review of documents and other evidence; my conversations with other law enforcement personnel; and my training, experience and advice received concerning the use of computers in criminal activity and the forensic analysis of electronically stored information ("ESI"). Because this Affidavit is being submitted for the limited purpose of establishing probable cause, it does not include all the facts that I have learned during the course of my investigation. Where the contents of documents and the actions, statements, and conversations of others are reported herein, they are reported in substance and in part, except where otherwise indicated.

B. The Subject Offenses

6. For the reasons detailed below, I believe that there is probable cause to believe that the Subject Devices also contain evidence, fruits, and instrumentalities of (i) violations of Title 18, United States Code, Section 2252 (possession, transportation, receipt, distribution, production, and reproduction of sexually explicit material relating to children) and Title 18, United States Code, Section 2252A (activities relating to material constituting or containing child pornography) (the "CP Offenses"); and (ii) violations of Title 17, United States Code, Section 506 and Title 18, United States Code, Section 2319 (criminal infringement of a copyright) (the "Copyright Offenses").

C. Terminology

7. The term "computer," as used herein, is defined as set forth in Title 18, United States Code, Section 1030(e)(1).

8. The terms "records," "documents," and "materials" include all information recorded in any form, visual or oral, and by any means, whether in handmade form (including, but

not limited to, writings, drawings, paintings), photographic form (including, but not limited to, microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, photocopies) or electrical, electronic or magnetic form (including, but not limited to, tape recordings, cassettes, compact discs, electronic or magnetic storage devices such as floppy diskettes, hard disks, CD-ROMs, digital video disks (DVDs), Personal Digital Assistants (PDAs), Multi Media Cards (MMCs), memory sticks, optical discs, printer buffers, smart cards, memory calculators, electronic dialers, Bernoulli drives, or electronic notebooks, as well as digital data files and printouts or readouts from any magnetic, electrical or electronic storage device), as well as the equipment needed to record such information (including but not limited to cameras and video recording and storage devices).

9. The term child pornography is defined in Title 18, United States Code, Section 2256(8) in pertinent part as "any visual depiction, including any photograph, film, video, picture, or computer or computer-generated image or picture, whether made or produced by electronic, mechanical, or other means, of sexually explicit conduct, where . . . the production of such visual depiction involves the use of a minor engaging in sexually explicit conduct."[1]

10. The terms "Minor," "Sexually Explicit Conduct" and "Visual Depiction" are defined as set forth in Title 18, United States Code, Section 2256.

II. Probable Cause Justifying Search of the Subject Devices

A. Probable Cause for Evidence of CP Offenses

11. On March 13, 2017, the Honorable Barbara C. Moses, a U.S. Magistrate Judge for the Southern District of New York, issued a search warrant (the "Schulte Search Warrant") to

[1] *See also Ashcroft* v. *Free Speech Coalition*, 535 U.S. 234 (2002) (analyzing constitutional validity of the definitions set forth in 18 U.S.C. § 2256(8)).

search the residence of JOSHUA ADAM SCHULTE located at 200 East 39th Street, Apartment 8C, New York, New York 10016 (the "Residence").[2] The Schulte Search Warrant was issued in connection with the investigation of the unauthorized dissemination on March 7, 2017, by wikileaks.org of documents and files that contained classified, national defense information belonging to the Central Intelligence Agency (the "Classified Materials"). As a result, the Schulte Search Warrant authorized the search of the Premises and any electronic devices found therein, for evidence, fruits, and instrumentalities of offenses relating to the unauthorized disclosure of the Classified Materials (the "Espionage Offenses").

12. On or about March 15, 2017, members of the FBI searched the Residence.[3] During the course of that search, law enforcement officers recovered, among other things, the Subject Devices, including multiple computers, servers, and other portable electronic storage devices.[4] Following the seizure of the Subject Devices, the devices were transported by the FBI for analysis and examination to a U.S. Government facility in Herndon, Virginia, within the Eastern District of Virginia, where they remain as of the date of this application.

13. Based on my conversations with members of the FBI who are involved in searching the Subject Devices for evidence, fruits, and instrumentalities of the Espionage Offenses pursuant to the terms of the Schulte Search Warrant, I have learned, among other things, that on or about April 7, 2017, a photograph was discovered on SCHULTE's desktop computer (the "Desktop

---

[2] A copy of the Schulte Search Warrant is attached as Exhibit A. A copy of the Affidavit in support of the Schulte Search Warrant is attached as Exhibit B and is incorporated herein by reference.

[3] The March 15, 2017 search of the Residence was pursuant to a second search warrant issued by the Honorable Barbara C. Moses on the same day as the search. The Government sought a second search warrant because the Schulte Search Warrant was executed covertly on or about March 14, 2017. However, the items to be searched and seized pursuant to the second search warrant were identical to that which is set forth in the Schulte Search Warrant attached to this Affidavit.

[4] A list of the Subject Devices is attached as Exhibit C.

Computer") that appears to depict child pornography (the "CP Picture"). The Desktop Computer appears to have been connected to other Subject Devices in the Residence, including several servers. As a result, data on the Desktop Computer was likely also accessible through, or available on, some of the other Subject Devices in the Residence.

14. Based on my conversations with FBI agents who have spoken to an agent who is assigned to the Crimes Against Children Squad (the "CACS Agent") and who has reviewed the CP Picture, I understand that the CP Picture appears to depict child pornography.[5] Specifically, the CACS Agent believes the CP Picture depicts a naked young child on all fours and what appear to be two adults around her, one of whom appears to be performing a sexual act on the child—oral sex around the child's buttocks. The CACS Agent also believes that the child is a minor based on, among other things, body structure, lack of breast development, and lack of pubic hair.[6]

---

[5] Based on my conversations with the CACS Agent, I understand that it is possible that the CP Picture (like many photographs of child pornography) could be altered and not a real picture. However, the CACS Agent had only reviewed a printout of the CP Picture. Members of the FBI who analyzed the Desktop Computer have informed me that the CP Picture looks more like an actual photo when viewed on the computer as opposed to when printed. I know that an agent involved in this investigation has viewed the CP Picture on the Desktop Computer and concluded that it is an actual photograph.

[6] On or about April 14, 2017, the Honorable Theresa C. Buchanan, United States Magistrate Judge, Eastern District of Virginia, issued a search warrant (the "April 14 Search Warrant") identical in part to that sought here, *i.e.*, expanding the scope of the search of the Subject Devices to include evidence, fruits, and instrumentalities of the CP Offenses. The April 14 Search Warrant also expanded the search of the Subject Devices to include evidence, fruits, and instrumentalities of the Copyright Offenses. The probable cause set forth in support of the April 14 Search Warrant—as it related to the CP Offenses only (*i.e.*, not the Copyright Offenses)—relied in part on evidence obtained from the results of a prior search warrant issued on or about March 14, 2017 in the Southern District of New York pursuant to the Stored Communications Act, 18 U.S.C. § 2703 (the "SCA Search Warrant"). I have recently learned that, although the SCA Search Warrant limited the scope of that search to evidence, fruits, and instrumentalities of the Espionage Offenses, while executing that search, agents also conducted a limited search for evidence relating to child pornography, and such evidence was used in support of the April 14 Search Warrant application to expand the search of the Subject Devices to include evidence, fruits, and instrumentalities of the CP Offenses. The limited search related to child pornography occurred after prosecutors made

15. Based on my training, experience, and discussions with other FBI agents, I know that persons who collect and distribute child pornography frequently collect and view sexually explicit materials in a variety of media, such as photographs, magazines, motion pictures, video tapes, books, slides and/or drawings or other visual media that they use for their own sexual arousal and gratification. These examples of visual media containing sexually explicit materials are often times stored on various devices, such as the Subject Devices, including but not limited to, computers, disk drives, servers, modems, thumb drives, personal digital assistants, mobile phones and smart phones, digital cameras, and scanners, and the data within the aforesaid objects relating to said materials.

16. In addition, I know that individuals who collect and distribute child pornography, in the event that they change computers, will often back up or transfer files from their old computers' hard drives to that of their new computers, so as not to lose data, including that described in the foregoing paragraph, which would be valuable in facilitating their criminal activity. In addition, individuals who engage in such criminal activity will often also store or transfer files on electronic storage media other than computer hard drives, including thumb drives, flash memory cards, CD-ROMs, or portable hard drives to, for example, facilitate the use of the information or to transfer it to co-conspirators in support of the criminal scheme.

---

the decision to obtain a new, expanded search warrant based upon the April 7, 2017 discovery of suspected child pornography on the Desktop Computer, described above. Although I believe that there was ample probable cause set forth in the April 14 Warrant application—separate and apart from the limited evidence obtained from the SCA Search Warrant cited therein—to justify an expanded search of the Subject Devices for evidence, fruits and instrumentalities of the CP Offenses, out of an abundance of caution, and because the search of the Subject Devices (which consists of numerous terabytes of data) is only partially complete, I am submitting this renewed application, which does not rely in any way on the evidence obtained from the SCA Warrant. In the interim, agents have been instructed by the Assistant United States Attorneys involved in this investigation to stop any searches related to the CP Offenses absent renewed additional authorization under Rule 41 of the Federal Rules of Criminal Procedure.

17. I also know that the child pornography detailed above was likely downloaded via the Internet using the Desktop Computer or other of the Subject Devices. As a result, the Desktop Computer and other Subject Devices may contain messages, emails, photographs, and/or videos relating to the possession, receipt, or production of child pornography. Computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a hard drive, deleted, or viewed via the Internet. Electronic files can be stored on a hard drive for years at little or no cost. Even when such files have been deleted, they can often be recovered, depending on how the hard drive has subsequently been used, months or years later with forensics tools. Specifically, when a person "deletes" a file on a home computer, the data contained in the file does not actually disappear; rather, that data remains on the hard drive until it is overwritten by new data. Deleted files, or remnants of deleted files, may accordingly reside in "slack space" (space that is not being used for storage of a file) for long periods of time before they are overwritten. In addition, a computer's operating system may keep a record of deleted data in a "swap" or "recovery" file. Similarly, files that have been viewed via the Internet are generally automatically downloaded into a temporary Internet directory or "cache." The browser typically maintains a fixed amount of hard drive space devoted to these files, and the files are only overwritten as they are replaced with more recently viewed Internet pages. Thus, the ability to retrieve from a hard drive or other electronic storage media depends less on when the file was downloaded or viewed than on a particular user's operating system, storage capacity, and computer habits.

18. Based on the foregoing, I respectfully submit there is probable cause to believe that JOSHUA ADAM SCHULTE has engaged in the CP Offenses, and that evidence of this criminal activity is likely to be found on the Subject Devices. As a result, I am seeking authorization for a

search warrant to search the Subject Devices for evidence of the CP Offenses. This includes, as set forth in Attachment A, the following:

- Evidence of computer programs used to access, transmit, or store information relating to the CP Offenses;
- Evidence of counter-forensic programs (and associated data) that are designed to eliminate data from computer devices, storage media, and related electronic equipment;
- Evidence of visual or written depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256(2);
- Motion pictures, films, videos, and other recordings of visual or written depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256(2);
- Correspondence and records pertaining to violation of the CP Offenses including, but not limited to electronic mail, chat logs, electronic messages, and records bearing on the production, reproduction, receipt, shipment, orders, requests, trades, purchases, or transactions involving any visual depiction of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256(2);
- Records or other items which evidence ownership, control, or use of, or access to computer devices, storage media, and related electronic equipment used to access, transmit, or store information relating to the CP Offenses, including but not limited to sales receipts, warranties, bills for internet access, registry entries, configuration files, saved usernames and passwords, user profiles, email contacts, and photographs.
- Information or correspondence pertaining to affiliation with any child exploitation bulletin boards, chat forums, or organizations;
- Any child pornography as defined by 18 U.S.C. § 2256(8);
- Any child erotica, defined as suggestive visual depictions of nude minors which do not constitute child pornography as defined by 18 U.S.C. § 2256(8) or visual depictions of minors engaged in sexually explicit conduct as defined by 18 U.S.C. § 2256(2);
- Notes, documents, records, invoices, or correspondence, in any format and medium, including, but not limited to, e-mail messages, chat logs and electronic messages, other digital data files and web cache information, related to the possession, distribution, receipt, or production of, or access with intent to view, child pornography as defined in 18 U.S.C. § 2256(8), or visual depictions of minors engaged in sexually explicit conduct as defined in 18 U.S.C. § 2256(2);
- Names, and lists of names and addresses of individuals (including minors) related to the possession, distribution, receipt, or production of, or access with intent to view, child

pornography as defined in 18 U.S.C. § 2256(8), or visual depictions of minors engaged in sexually explicit conduct as defined in 18 U.S.C. § 2256(2);

- Mailing lists and/or supplier lists related to the possession, distribution, receipt, or production of, or access with intent to view, child pornography as defined in 18 U.S.C. § 2256(8), or visual depictions of minors engaged in sexually explicit conduct as defined in 18 U.S.C. § 2256(2); and

- Financial records, including credit card information, bills, and payment records related to related to the possession, distribution, receipt, or production of, or access with intent to view, child pornography as defined in 18 U.S.C. § 2256(8), or visual depictions of minors engaged in sexually explicit conduct as defined in 18 U.S.C. § 2256(2)

19. This application also requests authorization to search the ESI on the Subject Devices pursuant to the same procedures as set forth in the Schulte Search Warrant. (*See* Schulte Search Warrant Application, Part IV.)

B. Probable Cause for Evidence of Copyright Offenses

20. Based on my conversations with members of the FBI who are involved in searching the Subject Devices for evidence, fruits, and instrumentalities of the Espionage Offenses pursuant to the terms of the Schulte Search Warrant, I have learned, among other things, that at least one of the servers recovered from the Residence ("Server-1") has indications that SCHULTE was involved in illegally sharing copyrighted movies over the Internet. Specifically, Server-1's command log (which shows the history of commands sent to Server-1 by the user, likely via a computer connected to Server-1), indicates that SCHULTE participated in the sharing of dozens of movies using "torrent trackers."[7] Based on my training, experience and conversations with others, I understand that torrent trackers are computer code (or a "protocol") that connects

[7] Upon viewing the command log, which was searched pursuant to the terms of the Schulte Search Warrant for evidence regarding the Espionage Offenses, and upon seeing indications of illegal movie sharing, members of the FBI stopped viewing the command log and contacted the U.S. Attorney's Office.

computers on the Internet to each other in order to facilitate the transfer of large files over the Internet.

21. Based on my training, experience, and my review of the public catalog of copyrighted works available through the United States Copyright Office, I know that most, if not all, of the movies that SCHULTE appears to have participated in sharing are copyrighted works registered with the United States Copyright Office. For example, among the many movies that were apparently shared include *Hacksaw Ridge*; *The Revenant*; *Captain America: Civil War*; and *The Hateful Eight*, all of which are copyrighted works currently registered with the United States Copyright Office.

22. In or about March 2017, FBI agents conducted interviews of multiple CIA employees who know SCHULTE. Among other things, one of those employees stated that SCHULTE operates a service allowing users to stream movies over the internet (the "Streaming Service") and that SCHULTE manages the accounts of users of the Streaming Service.

23. Based on my review of a telephone that was among the Subject Devices for evidence, fruits, and instrumentalities of the Espionage Offenses pursuant to the terms of the Schulte Search Warrant, I have learned, among other things, that on or about October 31, 2016, SCHULTE sent an email to approximately 20 other individuals with the subject line "Pedbsktbll Plex Server Downtime 11/9/2016-1/2017" (the "Email"). In the Email, SCHULTE notifies the recipients that the "server will be down as it relocates to NYC starting 11/9. Thus, you will have the next 9 days to select and download material you may wish to watch during that downtime. Hopefully, the server will be back and running mid to late December – January at the latest." Based on my training, experience, and participation in this investigation, I believe that SCHULTE

was referring to the Streaming Service and was alerting users that the service would be unavailable while he moved to New York in late 2016.

24. Based on my training, experience, and discussions with other FBI agents, I know that persons who engage in the illegal transmission, distribution, and receipt of copyrighted workers typically store evidence of such works on various devices, such as the Subject Devices, including but not limited to, computers, disk drives, servers, modems, thumb drives, personal digital assistants, mobile phones and smart phones, digital cameras, and scanners, and the data within the aforesaid objects relating to said materials.

25. In addition, I know that individuals who engage in the illegal distribution of copyrighted workers, in the event that they change computers, will often back up or transfer files from their old computers' hard drives to that of their new computers, so as not to lose data, including that described in the foregoing paragraph, which would be valuable in facilitating their criminal activity. Furthermore, individuals who engage in such criminal activity will often also store or transfer files on electronic storage media other than computer hard drives, including thumb drives, flash memory cards, CD-ROMs, or portable hard drives to, for example, facilitate the use of the information or to transfer it to co-conspirators in support of the criminal scheme.

26. I also know that the movies detailed above were likely downloaded via the Internet using Server-1 and other of the Subject Devices. As a result, Server-1 and other Subject Devices may contain messages, emails, and/or videos relating to the transmission, distribution, and receipt of copyrighted works. As noted above, computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a hard drive, deleted, or viewed via the Internet.

27. Based on the foregoing, I respectfully submit there is also probable cause to believe that JOSHUA ADAM SCHULTE has engaged in the Copyright Offenses, and that evidence of this criminal activity is likely to be found on the Subject Devices. I am also seeking authorization for a search warrant to search the Subject Devices for evidence of the Copyright Offenses. Specifically, this includes, as set forth in Attachment A, the following:

- Evidence of computer programs used to transmit or store information relating to the Copyright Offenses;
- Evidence of counter-forensic programs (and associated data) that are designed to eliminate data from computer devices, storage media, and related electronic equipment;
- Evidence of copyrighted works, including motion pictures, films, videos, other recordings, and documents relating to the Copyright Offenses;
- Correspondence and records pertaining to violation of the Copyright Offenses including, but not limited to electronic mail, chat logs, electronic messages, and records bearing on the transmission, receipt, and/or storage of copyrighted works;
- Records or other items which evidence ownership, control, or use of, or access to computer devices, storage media, and related electronic equipment used to transmit or store information relating to the Copyright Offenses, including but not limited to sales receipts, warranties, bills for internet access, registry entries, configuration files, saved usernames and passwords, user profiles, email contacts, and photographs.
- Any copyrighted works;
- Notes, documents, records, invoices, or correspondence, in any format and medium, including, but not limited to, e-mail messages, chat logs and electronic messages, other digital data files and web cache information, related to the transmission, receipt, and/or storage of copyrighted works;
- Names, and lists of names and addresses of individuals (including minors) related to the transmission, receipt, and/or storage of copyrighted works;
- Mailing lists and/or supplier lists related to the transmission, receipt, and/or storage of copyrighted works; and
- Financial records, including credit card information, bills, and payment records related to the transmission, receipt, and/or storage of copyrighted works.

28. This application also requests authorization to search the ESI on the Subject Devices pursuant to the same procedures as set forth in the Schulte Search Warrant. (*See* Schulte Search Warrant Application, Part IV.)

III. Conclusion and Ancillary Provisions

29. Based on the foregoing, I respectfully request the court to issue a warrant to search the items and information specified in Attachment A to this Affidavit and to the Search and Seizure Warrant. In light of the confidential nature of the continuing investigation, I respectfully request that this Affidavit and all papers submitted herewith be maintained under seal until the Court orders otherwise.

Garrett L. Igo
Special Agent
Federal Bureau of Investigation

Sworn to and signed before me on
this 10th day of May 2017

/s/
Michael S. Nachmanoff
United States Magistrate Judge

Michael S. Nachmanoff
United States Magistrate Judge

Attachment A

I. Devices to be Searched—Subject Devices

The devices to be searched (the "Subject Devices") include any and all electronic devices seized pursuant to a search warrant executed on or about March 15, 2017 at the premises described as apartment 8C in a building located at 200 East 39th Street, New York, New York 10016.

II. The Search of the Subject Devices

A. Evidence, Fruits, and Instrumentalities of the Child Pornography Offenses

The Subject Devices may be searched for the following evidence, fruits, and/or instrumentalities of violations of Title 18, United States Code, Sections 2252 (activities relating to material constituting or containing child pornography) and 2252A (possession, transportation, receipt, distribution, production, and reproduction of sexually explicit material relating to children) (the "CP Offenses"):

- Evidence of computer programs used to access, transmit, or store information relating to the CP Offenses;
- Evidence of counter-forensic programs (and associated data) that are designed to eliminate data from computer devices, storage media, and related electronic equipment;
- Evidence of visual or written depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256(2);
- Motion pictures, films, videos, and other recordings of visual or written depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256(2);
- Correspondence and records pertaining to violation of the CP Offenses including, but not limited to electronic mail, chat logs, electronic messages, and records bearing on the production, reproduction, receipt, shipment, orders, requests, trades, purchases, or transactions involving any visual depiction of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256(2);
- Records or other items which evidence ownership, control, or use of, or access to computer devices, storage media, and related electronic equipment used to access, transmit, or store information relating to the CP Offenses, including but not limited to sales receipts, warranties, bills for internet access, registry entries, configuration files, saved usernames and passwords, user profiles, email contacts, and photographs.

- Information or correspondence pertaining to affiliation with any child exploitation bulletin boards, chat forums, or organizations;

- Any child pornography as defined by 18 U.S.C. § 2256(8);

- Any child erotica, defined as suggestive visual depictions of nude minors which do not constitute child pornography as defined by 18 U.S.C. § 2256(8) or visual depictions of minors engaged in sexually explicit conduct as defined by 18 U.S.C. § 2256(2);

- Notes, documents, records, invoices, or correspondence, in any format and medium, including, but not limited to, e-mail messages, chat logs and electronic messages, other digital data files and web cache information, related to the possession, distribution, receipt, or production of, or access with intent to view, child pornography as defined in 18 U.S.C. § 2256(8), or visual depictions of minors engaged in sexually explicit conduct as defined in 18 U.S.C. § 2256(2);

- Names, and lists of names and addresses of individuals (including minors) related to the possession, distribution, receipt, or production of, or access with intent to view, child pornography as defined in 18 U.S.C. § 2256(8), or visual depictions of minors engaged in sexually explicit conduct as defined in 18 U.S.C. § 2256(2);

- Mailing lists and/or supplier lists related to the possession, distribution, receipt, or production of, or access with intent to view, child pornography as defined in 18 U.S.C. § 2256(8), or visual depictions of minors engaged in sexually explicit conduct as defined in 18 U.S.C. § 2256(2); and

- Financial records, including credit card information, bills, and payment records related to related to the possession, distribution, receipt, or production of, or access with intent to view, child pornography as defined in 18 U.S.C. § 2256(8), or visual depictions of minors engaged in sexually explicit conduct as defined in 18 U.S.C. § 2256(2).

B. Evidence, Fruits, and Instrumentalities of the Copyright Offenses

The Subject Devices may also be searched for the following evidence, fruits, and/or instrumentalities of violations of violations of 17 U.S.C. § 506 and 18 U.S.C. § 2319 (criminal infringement of a copyright) (the "Copyright Offenses"):

- Evidence of computer programs used to transmit or store information relating to the Copyright Offenses;

- Evidence of counter-forensic programs (and associated data) that are designed to eliminate data from computer devices, storage media, and related electronic equipment;

- Evidence of copyrighted works, including motion pictures, films, videos, other recordings, and documents relating to the Copyright Offenses;

- Correspondence and records pertaining to violation of the Copyright Offenses including, but not limited to electronic mail, chat logs, electronic messages, and records bearing on the transmission, receipt, and/or storage of copyrighted works;

- Records or other items which evidence ownership, control, or use of, or access to computer devices, storage media, and related electronic equipment used to transmit or store information relating to the Copyright Offenses, including but not limited to sales receipts, warranties, bills for internet access, registry entries, configuration files, saved usernames and passwords, user profiles, email contacts, and photographs.

- Any copyrighted works;

- Notes, documents, records, invoices, or correspondence, in any format and medium, including, but not limited to, e-mail messages, chat logs and electronic messages, other digital data files and web cache information, related to the transmission, receipt, and/or storage of copyrighted works;

- Names, and lists of names and addresses of individuals (including minors) related to the transmission, receipt, and/or storage of copyrighted works;

- Mailing lists and/or supplier lists related to the transmission, receipt, and/or storage of copyrighted works; and

- Financial records, including credit card information, bills, and payment records related to the transmission, receipt, and/or storage of copyrighted works.

C. Review of ESI

In conducting a review of ESI on the Subject Devices, law enforcement personnel may use various techniques, including but not limited to:

- surveying various file "directories" and the individual files they contain (analogous to looking at the outside of a file cabinet for the markings it contains and opening a drawer believed to contain pertinent files);

- opening or cursorily reading the first few "pages" of such files in order to determine their precise contents;

- scanning storage areas to discover and possibly recover recently deleted files;

- scanning storage areas for deliberately hidden files;

- performing key word searches through all electronic storage areas to determine whether occurrences of language contained in such storage areas exist that are intimately related to the subject matter of the investigation; and

- making reasonable efforts to utilize computer search methodology to search only for files, documents, or other electronically stored information within the categories identified in Section II.A of this Attachment.

Law enforcement personnel will make reasonable efforts to search only for files, documents, or other electronically stored information within the categories identified in Section II.A and II.B. of this Attachment. However, law enforcement personnel are authorized to conduct a complete review of all ESI from the Subject Devices if necessary to evaluate its contents and to locate all data responsive to the warrant.

IN THE UNITED STATES DISTRICT COURT FOR THE

EASTERN DISTRICT OF VIRGINIA

Alexandria Division

IN THE MATTER OF THE SEARCH OF: Electronic Devices Previously Seized from the Premises of 200 East 39th Street, Apartment 8C, New York, NY 10016	))))	**UNDER SEAL** Case No. 1:17-SW243

GOVERNMENT'S MOTION TO SEAL SEARCH WARRANT
PURSUANT TO LOCAL RULE 49(B)

The United States of America, by and through undersigned counsel, upon the return of its executed search warrant,[1] and pursuant to Local Rule 49(B) of the Local Criminal Rules for the United States District Court for the Eastern District of Virginia, now asks for an Order to Seal the search warrant, application for the search warrant and the affidavit in support of the search warrant, together with this Motion to Seal and proposed Order, until the United States makes a motion to unseal the search warrant and affidavit.

I. REASONS FOR SEALING (See Local Rule 49(B)(1))

1. At the present time, Special Agents of the Federal Bureau of Investigation (FBI) are conducting an investigation into: (i) violations of Title 18, United States Code, Section 2252 (possession, transportation, receipt, distribution, production, and reproduction of sexually explicit material relating to children) and Title 18, United States Code, Section 2252A (activities relating to material constituting or containing child pornography); and (ii) violations of Title 17, United States Code, Section 506 and Title 18, United States Code, Section 2319 (criminal infringement of a copyright).

---

[1] Pursuant to Local Rule 49(B), "[n]o separate motion to seal is necessary to seal a search warrant *from the time of issuance to the time the executed warrant is returned.*" (Emphasis added.) This is because, as Rule 49(B) additionally mandates, "[u]ntil an executed search warrant is returned, search warrants and related papers are not filed with the Clerk."

2. Premature disclosure of the specific details of this ongoing investigation (as reflected, for example, in the affidavit in support of search warrant) would jeopardize this continuing criminal investigation and may lead to the destruction of additional evidence in other locations. Thus, a sealing order is necessary to avoid hindering the ongoing investigation in this matter.

3. The United States has considered alternatives less drastic than sealing, including, for example, the possibility of redactions, and has determined that none would suffice to protect this investigation.

II. THE GOVERNING LAW (See Local Rule 49(B)(2))

4. It is generally recognized that the public has a common law right of access, but not a First Amendment right of access, to judicial documents, including documents associated with *ex parte* proceedings such as search warrant affidavits. Media General Operations, Inc. v. Buchanan, 417 F.3d 424, 429 (4th Cir. 2005); In re Washington Post Company v. Hughes, 923 F.2d 324, 326 (4th Cir. 1991). "But the right of access is qualified, and a judicial officer may deny access to search warrant documents if sealing is 'essential to preserve higher values' and 'narrowly tailored to serve that interest.'" Media General Operations, 417 F.3d at 429 (citations omitted); see also In re Knight Pub. Co., 743 F.2d 231, 235 (4th Cir. 1984) ("[t]he trial court has supervisory power over its own records and may, in its discretion, seal documents if the public's right of access is outweighed by competing interests"). Sealing search warrants and their accompanying affidavits and application is within the discretionary powers of a judicial officer where, among other things, an "'affidavit contain[s] sensitive details of an ongoing investigation' and it is 'clear and apparent from the affidavits that any disclosure of the

information there would hamper' th[e] ongoing investigation." Media General Operations, 417 F.3d at 430 (citations omitted); see also In re Search Warrant for Matter of Eye Care Physicians of America, 100 F.3d 514, 518 (7th Cir. 1996).

5. Before a district court generally may seal judicial records or documents, it must (a) provide public notice of the request to seal and allow interested parties a reasonable opportunity to object, (b) consider less drastic alternatives to sealing the documents, and (c) provide specific reasons and factual findings supporting its decision to seal the documents and for rejecting the alternatives. Ashcraft v. Conoco, Inc., 218 F.3d 288, 302 (4th Cir. 2000).

6. However, regarding the notice requirement in the specific context of a search warrant, the Fourth Circuit has cautioned that "the opportunity to object" cannot "arise prior to the entry of a sealing order when a search warrant has not been executed." Media General Operations, 417 F.3d at 429. "A rule to the contrary would endanger the lives of officers and agents and allow the subjects of the investigation to destroy or remove evidence before the execution of the search warrant." Id.; see also Franks v. Delaware, 438 U.S. 154, 169 (1978). Accordingly, in the context of search warrants, "the notice requirement is fulfilled by docketing 'the order sealing the documents,' which gives interested parties the opportunity to object after the execution of the search warrants." Media General Operations, 417 F.3d at 430 (quoting Baltimore Sun Co. v. Goetz, 886 F.2d 60, 65 (4th Cir. 1989)); see also Local Rule 49(B) ("Until an executed search warrant is returned, search warrants and related papers are not filed with the Clerk.").

7. As to the requirement of a court's consideration of alternatives, the Fourth Circuit counsels that, "[i]f a judicial officer determines that full public access is not appropriate, she 'must consider alternatives to sealing the documents,' which may include giving the public

access to some of the documents or releasing a redacted version of the documents that are the subject to the government's motion to seal." Media General Operations, 417 F.3d at 429 (quoting Goetz, 886 F.2d at 66).

8. Finally, regarding the requirement of specific findings, the Fourth Circuit's precedents state that, "'in entering a sealing order, a 'judicial officer may explicitly adopt the facts that the government presents to justify sealing when the evidence appears creditable,'" Media General Operations, 417 F.3d at 429 (quoting Goetz, 886 F.2d at 65), so long as the ultimate "decision to seal the papers" is "made by the judicial officer," Goetz, 886 F.2d at 65. "Moreover, if appropriate, the government's submission and the [judicial] officer's reason for sealing the documents can be filed under seal." Goetz, 886 F.2d at 65; see also In re Washington Post Co., 807 F.2d 383, 391 (4th Cir. 1986) ("if the court concludes that a denial of public access is warranted, the court may file its statement of the reasons for its decision under seal").

III. PERIOD OF TIME GOVERNMENT SEEKS TO HAVE MATTER REMAIN UNDER SEAL (See Local Rule 49(B)(3))

9. Pursuant to Local Rule 49(B)(3), the search warrant and the affidavit will remain sealed until the need to maintain the confidentiality of the search warrant application and the related investigation expires, after which time the United States will move to unseal the search warrant and affidavit.

WHEREFORE, the United States respectfully requests that the search warrant, application for search warrant, affidavit in support of the search warrant, and this Motion to Seal and proposed Order be sealed until further Order of the Court.

Respectfully submitted,

Dana J. Boente
United States Attorney

By: W. Neil Hammerstrom
W. Neil Hammerstrom, Jr.
Assistant United States Attorney

IN THE UNITED STATES DISTRICT COURT FOR THE

EASTERN DISTRICT OF VIRGINIA

Alexandria Division

IN THE MATTER OF THE SEARCH OF: Electronic Devices Previously Seized from the Premises of 200 East 39th Street, Apartment 8C, New York, NY 10016	))))	**UNDER SEAL** Case No. 1:17-SW-243

ORDER TO SEAL

The UNITED STATES, pursuant to Local Rule 49(B) of the Local Criminal Rules for the United States District Court for the Eastern District of Virginia, having moved to seal the search warrant, the application for search warrant, the affidavit in support of the search warrant, the Motion to Seal, and proposed Order in this matter; and

The COURT, having considered the government's submissions, including the facts presented by the government to justify sealing; having found that revealing the material sought to be sealed would jeopardize an ongoing criminal investigation; having considered the available alternatives that are less drastic than sealing, and finding none would suffice to protect the government's legitimate interest in concluding the investigation; and having found that this legitimate government interest outweighs at this time any interest in the disclosure of the material; it is hereby

ORDERED, ADJUDGED, and DECREED that, the search warrant, application for search warrant, affidavit in support of the search warrant, Motion to Seal, and this Order be sealed until further Order of the Court.

/s/
Michael S. Nachmanoff
United States Magistrate Judge

Michael S. Nachmanoff
United States Magistrate Judge

Date: 5/10/17
Alexandria, Virginia